



TRUSTED INFORMATION SYSTEMS, INC.

Building a World of TrustSM

February 11, 1997

STEPHEN T. WALKER
PRESIDENT

Ms. Nancy Crowe
Regulatory Policy Division, Room 2705
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Avenue, N.W.
Washington, DC 20230

Dear Ms. Crowe:

Trusted Information Systems, Inc. ("TIS") would like to thank you for the opportunity to comment on the interim rule "Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List" (61 Federal Register 68572-68587) that exercised jurisdiction over certain encryption items formerly on the U.S. Munitions List. The interim rule as published on 30 December 1996 makes substantial and significant progress toward making strong U.S. encryption products available worldwide and sustaining the economic competitiveness of U.S. firms. Given the short time frame between the October 1, 1996 Administration announcement and the promulgation of the rule, the various agencies are to be commended for the effort and energy devoted to passage of the regulation in a timely manner.

Furthermore, TIS appreciates the extent to which the new "interim relief" provisions for 56-bit, non-recovery encryption products improve the current competitive position of U.S. industry. TIS is already taking advantage of its new ability to ship its 56-bit non-recovery encryption products to its overseas market.

TIS especially appreciates the Commerce Department's recognition of the importance of the issues and stakes involved in establishing this new control regime and your willingness to consider comments from industry and the public in developing the final regulations. Such openness is crucial because the 30 December 1996 regulations do have some significant gaps and unresolved issues concerning:

- (1) export of key-recovery technologies and technical data;
- (2) export of key-recovery infrastructure products and technologies;
- (3) classification, export, and licensing of encryption and key-recovery encryption services, consulting, and training activities that formerly were controlled as "defense services" and for which "EI" controls are now being established; and
- (4) key-recovery agent certification and product classification.

TIS's comments on these are provided below, for your consideration and use. In addition, we offer suggestions on how to streamline the key-recovery encryption product classification process with respect to designation of approved key-recovery agents. TIS believes that proper attention to these areas will further the new regulations' objectives of improving the security of the global information infrastructure, sustaining the economic vitality and competitiveness of U.S. industry, and encouraging worldwide use of key-recovery encryption items within a key management infrastructure that "promote[s] electronic commerce and secure communications while protecting national security and public safety."

(1) Key-Recovery Technologies and Technical Data

The 30 December 1996 interim rule places "technology" for the "development," "production," or "use" of items controlled by ECCN 5A002 or ECCN 5D002 under the ECCN 5E002 [61 Federal Register 68587]. Specific mention is made of "**Encryption** software [emphasis added] controlled for EI reasons," which presumably could qualify for License Exception KMI under 5D002. However, the interim rule is silent on the licensing treatment of key-recovery technologies and technical data related to the development or production of key-recovery features, when such technologies and data do not include encryption software or executable code. Therefore, it is unclear what License Exception(s), if any, were intended to be available for key-recovery technology and technical data. As the regulation is currently written, License Exception "KMI" is not available for 5E002.

If the Commerce Department and BXA have the objective of fostering the widespread acceptance and use of key-recovery encryption products within a worldwide key management infrastructure, then it is a straightforward conclusion that making key-recovery (not just key-recovery encryption) technologies and technical data as widely available as possible will promote that objective. Similarly, controls on key-recovery technologies and technical data that require (or even suggest) case-by-case, customer-by-customer export and re-export review by BXA will unnecessarily impede that proliferation objective and needlessly inhibit adoption of U.S.-origin key recovery technologies by manufacturers and consumers outside the United States.

Encryption products are currently manufactured worldwide. In fact, as of December, 1996, TIS has identified 570 encryption products manufactured in 28 countries *other than the United States*. These products do not contain key recovery mechanisms that meet U.S. Government export requirements. If the goal of the U.S. Government is to encourage the transition to key-recovery encryption products, the non-U.S. companies that produce encryption products should have ready access to the best key-recovery mechanisms available—with no strings attached. Otherwise, these companies will continue to produce only non-key-recovery products.

Therefore, we recommend that key-recovery technologies and technical data (provided in electronic form) be given at least as liberal export/re-export treatment as key-recovery

encryption items are given—e.g., License Exception “KMI” should be available for export and re-export after a one-time classification review by BXA

(2) Key-Recovery Infrastructure Products and Technologies

As the interim rule correctly anticipates, establishment of the infrastructures for key recovery and for key management overall will take time and involve substantial market uncertainties as to rates of technology development and adoption. Establishment of key-recovery infrastructures will be advanced by liberal export treatment of the infrastructure products (e.g., Key Recovery Centers) and technologies (e.g., technical data pertaining to Key Recovery Centers).

At present, unless these products qualify for License Exception “KMI” as “key-recovery encryption products,” it is not clear that alternatives to case-by-case export and re-export review by BXA are available. As noted above, the situation for “key-recovery infrastructure technologies” is at best unclear. We suggest that liberal treatment analogous to License Exception “KMI” after one-time classification review is necessary in order to promote establishment and use of key recovery agents and other infrastructure components worldwide, to be used in conjunction with key-recovery encryption products of both U.S. and non-U.S. origin according to national and international law and agreements.

(3) Encryption and Key-Recovery Encryption Technical Assistance

The interim rule makes provision for certain technical assistance in conjunction with a product for which License Exception KMI is available, but specifics of the licensing requirements and processes for export of other technical services, consulting and training are not addressed. The framework within which activities that were formerly considered “defense services” under the U.S. Munitions List controls must be established so as not to burden exporters unduly through the delay inevitably caused by ambiguous requirements.

This need is particularly urgent for services and assistance that will enable non-US manufacturers to incorporate key recovery into their encryption products. Obviously, enabling these to be provided under liberal treatment analogous to License Exception “KMI” will promote widespread dissemination of key recovery. By contrast, continued uncertainties or overly restrictive licensing practices may retard international use of key recovery and most certainly will disadvantage U.S. companies.

(4) Key-Recovery Agent Certification and Product Classification

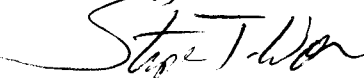
The procedures established under the interim rule couple availability of License Exception “KMI” with specifically designated key recovery agents. These are unnecessarily burdensome to manufacturers and consumers in that they anticipate case-by-case linkages between products and key recovery agents when classification requests are submitted.

As the number of BXA-approved (or approvable) key recovery agents increases, the current procedures will not scale well. Moreover, how consumers will be able to “switch” to different approved key recovery agents that offer recovery services on a commercial basis (thereby encouraging both price and quality competition among commercial agents) under the current procedures is unclear. TIS suggests approval of key recovery agents independent of the approval of specific products for export. This will allow key recovery agents to offer a wide range of services, and to compete with one another in the commercial marketplace. Indeed, it can lead to the creation of an entirely new industry (i.e., key recovery agent services).

Although specific products would not necessarily be “tied” permanently to a *specific* key recovery agent as a condition of exportability, Government interests will continue to be met, because each product must use a Government-approved key recovery agent in order to permit cryptographic functions to operate. It does not matter which one, as long as it is Government-approved. This permits user-choice consistent with Government requirements, and is illustrative of how technology created by the private sector, to serve a private sector purpose, can provide solutions that meet Government requirements *as an ancillary function*. In this case, commercial solutions can address specific Government interests without imposing unnecessary regulation or Government-centric design specifications.

Again, thank you for the opportunity to comment on the interim rule. If you have any questions regarding this submission, please contact Joan Winston at (703)356-2225 ext. 111 or Ken Mendelson at (301) 854-5348.

Sincerely,



Stephen T. Walker